Blockchain as a Catalyst for IoT Security

Sidharth Sunil[1], Anjum Zameer Bhat[1], Preethy Kurian[1] and Vikas Rao Naidu[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

The proliferation of IoT devices has created a critical need for secure communication and ownership of these devices. Digital signatures and public-key infrastructures are the traditional solutions that may be vulnerable to attacks, especially in large-scale IoT deployments. To address these issues, recent breakthrough technologies in the 4th Industrial Revolution are explored. The proposed research attempts to find solutions to secure IoT devices through Blockchain technology. Among the typical attacks in IoT devices, two major attacks including authentication and device ownership are considered in the present study. The former attack is handled by replacing the traditional credential stuffing approach with a more secure and user-friendly password-less login method through blockchain wallets. The latter attack is managed by implementing a smart contract in the Ethereum blockchain. In addition, novel approaches inspired by the works of Khalil et al 2023 and Arcenegui et al 2021 based on smart Non-Fungible Tokens (NFT) are explored. The proposed framework and solutions are beneficial for all stakeholders involved in IoT deployments, including device manufacturers, owners, and users. The proposed solution has several advantages for stakeholders, such as improved management of device identity, greater privacy and security, and lower expenses related to centralized management. Overall, the research proposes an optimistic approach for safeguarding IoT devices utilizing decentralized blockchain technology, which could promote a more secure and reliable IoT ecosystem.

Introduction

The Internet of Things (IoT) has become a potent paradigm for tying together a wide range of devices that share and transmit data online. By simplifying processes and enabling real-time access to data, IoT technology has changed several sectors, notably the medical, transport, and production sectors (Atzori et al., 2010). Considering their potential, IoT devices have grown quickly, raising serious issues related to privacy and security that have forced the creation of effective defenses (Granjal et al., 2015).

Traditional security technologies, including digital signatures and public-key infrastructures, have drawbacks when it comes to safeguarding IoT devices, especially while deploying them on a large scale (Sicari et al., 2015). Blockchain-based technology has come to prominence as a promising approach for dealing with IoT security concerns in recent times (Dorri et al., 2017). Blockchain, a decentralized and distributed ledger technology, provides data storage that is transparent, immutable, and safe (Christidis & Devetsikiotis, 2016). As a result, it is a good choice for boosting the privacy as well as security of IoT devices.

The current study focuses on two main attacks: authentication and device ownership-related attacks, with the goal of examining how blockchain technology might be used to improve IoT device security. The proposed framework offers an approach that enhances IoT device security while benefiting all stakeholders engaged in IoT deployments/implementation by utilizing blockchain wallets for password-less login and smart contracts which are Ethereum-based for managing ownership of devices.

Literature Review

Jia et al. (2020) proposed the A2 Chain, which decentralizes the handling of requests for authentication and lessens the load on the services that authenticate and the network by utilizing edge computing. The public key infrastruc-

ture (PKI) algorithm is replaced with the identity-based cryptography (IBC) algorithm in this method, which additionally employs sidechain and blockchain technologies in order to safely exchange the identity verification data of IoT devices across domains and reduce the administrative burden brought on by centralized authentication models. In light of this, it would appear that decentralized authentication models can enhance security and decrease congestion in massive IoT networks.

As part of a security-in-depth approach, Minoli and Occhiogrosso (2018) address the function of blockchain mechanisms (BCMs) in safeguarding IoT ecosystems. The research article demonstrates how blockchain technology can offer end-to-end security control for Internet of Things applications, highlighting the significance of a secure, shared public ledger in a variety of IoT situations, including Smart Grid, Intelligent Transportation Systems, and e-Health. This implies that adding blockchain technology as part of a more comprehensive security strategy can considerably improve the total safety of IoT systems.

Dorri et al. (2017) proposed an IoT-specific lightweight blockchain technology that removes the Proof of Work and the idea of currencies. The authors concentrated on the smart house tier and give every smart home a miner—a constantly online, high-resource device that handles all communication between inside and outside the home. For the purpose of monitoring and auditing conversations, the miner maintains a private and secure blockchain. The suggested framework's security regarding anonymity, reliability, and accessibility was carefully examined, and simulation results indicate that its overheads are negligible in comparison to its privacy and safety gains. The study contributes to the expanding body of knowledge in this field and suggests a feasible method for securing IoT networks utilizing blockchain technology.

A method to utilize blockchain technology for IoT device authentication is put forth by Dabhade and Tomar (2019). Their decentralized approach makes use of blockchain security qualities to tackle important IoT security challenges including identification of IoT devices, authentication, and data integrity while establishing safe virtual environments where devices may define and trust one another. After considering this work, utilizing blockchain technology for decentralized authentication can assist in addressing a few of the security issues that are present in IoT systems by nature.

Khalil et al. (2023) proposed the Decentralized Smart City of Things (DSCoT) architecture, which mixes fog computing and Non-Fungible Tokens (NFTs) for strong security characteristics like privacy, security, accessibility, and authorization. Their NFT-based blockchain design efficiently authenticates IoT-based smart devices utilized in smart cities, and studies of gas consumption and time complexity show how effective their architecture is. Reflecting on this, utilizing NFTs for authentication in IoT-based smart devices presents a distinctive and secure way to confirm device qualities and guarantee data security.

Methodology

The research study proposes a framework that utilizes blockchain technology for improving security in IoT devices. A methodology consisting of four steps is utilized to achieve the objective.

Step 1: Selection of Major Attacks

Two major attacks were identified as critical concerns for IoT devices: authentication and device ownership. These two areas were chosen for further exploration in the proposed framework.

Step 2: Implementation of Password-less Login Method

To address the authentication attack, a password-less login method was implemented using blockchain wallets. This method allows users to log in to their IoT devices without having to remember a password. Instead, their identity is verified using a private key associated with their blockchain wallet.

Step 3: Development of a Smart Contract on the Ethereum Blockchain

To address the device ownership attack, a smart contract was developed on the Ethereum blockchain. This smart contract allows the management of devices utilizing blockchain technology.

Step 4: Exploration of NFT-based Approaches

To further enhance device identity and ownership tracking, NFT-based approaches inspired by Khalil et al. (2023) were explored. This exploration allowed for the integration of NFTs into the proposed framework.

Overall, this methodology allowed for the development of a comprehensive framework that utilizes blockchain technology to improve the security of IoT devices. The subsequent section provides an overview of the proposed framework.

Proposed Framework

The proposed framework addresses the security issues of IoT devices by leveraging the capabilities of blockchain technology. The framework consists of three main components: password-less login, smart contract-based device ownership management, and NFT-based device identity and ownership tracking.

First, the suggested framework uses blockchain wallets to implement a password-free login method. Using blockchain wallets eliminates the need for passwords, which are frequently a weak area in conventional security measures, and enables safe user authentication. Instead, users will be able to verify their identity using their private key and blockchain wallet address.

Secondly, the system uses Ethereum blockchain smart contracts to control who owns what IoT devices. In smart contracts, the terms of the agreement between the buyer and seller are directly written into lines of code. These contracts self-execute. This makes it possible to manage device ownership in a transparent and safe manner because the blockchain securely stores ownership information that cannot be changed or interfered with.

Finally, the suggested framework also makes better use of NFTs for device identity and ownership monitoring. NFTs are distinctive digital assets that can be applied to signify ownership of tangible or intangible goods. The suggested framework can offer a better way of tracking device ownership and identity by modeling IoT devices as NFTs. Device theft and tampering can be avoided by using NFTs to provide a secure and transparent ownership history for each device.

The three elements are combined in the suggested framework to produce a safe and decentralized IoT ecosystem. The suggested framework provides a more secure authentication approach by doing away with the need for passwords and relying on the security of the blockchain. The ownership control of devices using smart contracts offers transparent and secure ownership management. Finally, using NFTs to track device identity and ownership offers a more dependable and impervious way to track device history.

Conclusion

The proposed study concludes by presenting a framework for enhancing IoT device security through the application of blockchain technology. Password-free login, smart contract-based device ownership management, and NFT-based device identity and ownership monitoring make up the framework's three core parts.

The suggested framework has several advantages over conventional security measures. The password-less login approach enhances security by doing away with the necessity for readily cracked passwords. By doing away with centralized management and lowering the possibility of an attack on a single point of failure, the decentralized device ownership management system enhances security. The management of device identity is improved overall thanks to the usage of NFTs, which improves device identity and ownership tracking.

Future Recommendations

Although the proposed framework has a lot of promise for enhancing IoT security, more study is required to identify its drawbacks and enhance its functionality. Future studies may focus on using sidechains and other blockchain technology to increase scalability and performance.

Further study may also investigate the usage of other digital assets, like tokens, to strengthen device identity and ownership monitoring. In this context, NFTs give several advantages, including the ability to provide unique device identification and ownership history. Future studies might investigate other applications for NFTs, like managing the supply chain for Internet of Things devices or updating device firmware.

Overall, the suggested approach represents a considerable improvement in IoT device security. To fully realize its potential and pinpoint areas for development, more study is required. By utilizing the capabilities of blockchain technology, the proposed framework has the potential to greatly enhance the security of IoT devices.

Acknowledgments

The research leading to the results has received funding from The Research Council (TRC) in the Sultanate of Oman under the Undergraduate Research Grant Program (TRC Grant Agreement No. BFP/URG/ICT/21/186).

References

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://www.sciencedirect.com/science/article/abs/pii/S1389128610001568?via%3Dihub

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Dabhade, J. D., & Tomar, D. S. (2019). An Approach to Authenticating Devise in IoT using Blockchain. *International Research Journal of Engineering and Technology (IRJET)*, *6*(7). https://www.irjet.net/archives/V6/i7/IRJET-V6I7167.pdf

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Jia, X., Hu, N., Yin, S., Zhao, Y., Zhang, C., & Cheng, X. (2020). A2 Chain: A Blockchain-Based Decentralized Authentication Scheme for 5G-Enabled IoT. *Mobile Information Systems*, 8889192. https://doi.org/10.1155/2020/8889192

Khalil, U., Malik, O. A., Ong, W. H., & Uddin, M. (2023). Dscot: An Nft-Based Blockchain Architecture for the Authentication of Iot-Based Smart Devices in Smart Cities. *Social Science Research Network.* https://doi.org/10.2139/ssrn.4355848

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1–2*, 1–13. https://doi.org/10.1016/j.iot.2018.05.002

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, Pages 146-164. https://doi.org/10.1016/j.comnet.2014.11.008